

<Priority Document Translation>

THE KOREAN INDUSTRIAL
PROPERTY OFFICE

This is to certify that annexed hereto is a true copy from the records of the Korean Industrial Property Office of the following application as filed.

Application Number : 2000-29631 (Patent)

Date of Application : May 31, 2000

Applicant(s) : HYUNDAI ELECTRONICS INDUSTRIES CO., LTD.

October 30, 2000

COMMISSIONER



대한민국 특허청
KOREAN INDUSTRIAL
PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto
is a true copy from the records of the Korean Industrial
Property Office.

출원번호 : 특허출원 2000년 제 31574 호
Application Number

출원년월일 : 2000년 06월 09일
Date of Application

출원인 : 현대전자산업주식회사
Applicant(s)

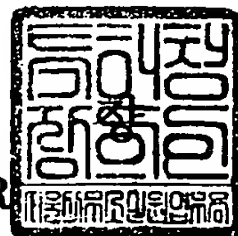
CERTIFIED COPY OF
PRIORITY DOCUMENT



2000 년 10 월 30 일

특 허 청

COMMISSIONER



【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【제출일자】	2000.05.31
【발명의 명칭】	데이터 암호화 표준 알고리즘을 이용한 암호화 장치
【발명의 영문명칭】	Encryption device using data encryption standard algorithm
【출원인】	
【명칭】	현대전자산업주식회사
【출원인코드】	1-1998-004569-8
【대리인】	
【성명】	박해천
【대리인코드】	9-1998-000223-4
【포괄위임등록번호】	1999-008448-1
【대리인】	
【성명】	원석희
【대리인코드】	9-1998-000444-1
【포괄위임등록번호】	1999-008444-1
【발명자】	
【성명의 국문표기】	임영원
【성명의 영문표기】	LIM, Young Won
【주민등록번호】	621128-1067119
【우편번호】	467-850
【주소】	경기도 이천시 대월면 현대전자사원아파트 106-1302
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사를 청구합니다. 대리인 박해천 (인) 대리인 원석희 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	0 면 0 원

1020000029631

2000/11/

【우선권주장료】	0	건	0	원
【심사청구료】	3	항	205,000	원
【합계】	234,000			원
【첨부서류】	1. 요약서·명세서(도면)_1통			

【요약서】**【요약】**

본 발명은 S-Box치환부를 4-포트의 입력을 가진 장치로 구현한 데이터 암호화 표준 알고리즘을 이용한 암호화 장치에 관한 것으로, 액세스(Access) 시간이 네 배 빠른 기억장치를 사용하여 주어진 시간에 데이터를 네 번 액세스하여 데이터 컨텐션(Contention)을 제거하고 면적을 최소화할 수 있는 암호화 방법 및 장치를 제공하는데 그 목적이 있다. 이를 위하여 본 발명은 데이터 암호화 표준 알고리즘을 사용하여 암호화를 수행하는 암호화 장치에 있어서, 제어기의 제어를 받아 입력되는 네 개의 48비트의 데이터 중에 하나를 선택하는 멀티플렉서; 상기 멀티플렉서에서 출력된 48비트 중에서 6비트의 어드레스 8 개를 입력받아 4비트의 데이터 8 개를 출력하는 8 개의 S-Box; 제어기의 제어를 받아 상기 4비트의 데이터를 네개로 분배하는 디멀티플렉서; 및 제1클럭과 제2클럭을 입력받아 상기 멀티플렉서와 디멀티플렉서를 제어하는 제어기를 포함하여 이루어진다.

【대표도】

도 6

【색인어】

멀티플렉서, S-Box, 디멀티플렉서, 제어기

【명세서】**【발명의 명칭】**

데이터 암호화 표준 알고리즘을 이용한 암호화 장치{Encryption device using data encryption standard algorithm}

【도면의 간단한 설명】

도1은 일반적인 DES 아키텍처의 사이퍼 함수와 S-Box 치환부의 상세한 구성도,
도2은 처리성능비를 증가시키는 4단의 파이프라인 구조를 갖는 종래기술의 DES 아키텍처의 블럭도,
도3은 종래기술에 따른 DES 아키텍처의 동작 순서를 나타내는 타이밍도,
도4는 종래기술의 DES 아키텍처의 파이프라인 동작 순서를 나타내는 타이밍도,
도5는 종래기술의 8단의 파이프라인 구조의 DES 아키텍처에서 단일 포트 S-Box 치환부의 구현 방식을 나타낸 상세한 블럭도,
도6은 본 발명의 8단의 파이프라인 DES 아키텍처에서 4-포트 S-Box 치환부의 구현을 나타낸 블럭도,
도7은 종래의 단일 포트 S-Box 치환부와 본 발명의 4-포트 S-Box 치환부의 동작을 나타내는 타이밍도.

* 도면의 주요 부분에 대한 부호의 설명 *

610 : 멀티플렉서

620 : S-Box

630 : 디멀티플렉서

640 : 제어기

【발명의 상세한 설명】**【발명의 목적】****【발명이 속하는 기술분야 및 그 분야의 종래기술】**

- <11> 본 발명은 암호화 장치에 관한 것으로, 특히 데이터 암호화 표준 알고리즘을 이용한 암호화 장치에 관한 것이다.
- <12> 일반적으로 데이터 암호화 표준(DES : Data Encryption Standard, 이하 DES라 칭함) 알고리즘은 가장 널리 쓰이고 있는 암호화 방식으로 네트워킹 사용이 증가함에 따라 그 중요성을 더해 가고 있다. 특히, 보안 인터넷 응용이나 원격 접근 서버나 케이블 모뎀과 위성용 모뎀 등의 분야에서 많이 이용되고 있다.
- <13> DES는 기본적으로 64비트 블록의 입력 및 출력을 가지는 64비트 블록 암호이며, 64비트의 키 블록 중 56비트가 암호화 및 복호화에 사용되고, 나머지 8비트는 패리티 검사용으로 사용된다. 또한, 64비트의 평문(Plain Text) 블록과 56비트의 키(Key)를 입력으로 해서 64비트의 암호문(Ciper Text) 블록을 출력하는 암호화 장치이다.
- <14> DES를 실현시키는 중요한 기법은 치환(P-Box), 대치(S-Box) 그리고 보조키(Subkey)를 발생시키는 키 스케줄 등이 있다.
- <15> 데이터 암호화부의 내부는 16라운드의 반복연산을 수행하는 형태로 되어 있고 입력부의 초기 치환(IP)와 출력부의 역초기 치환(IP⁻¹)으로 구성되어 있다.
- <16> 도1은 일반적인 DES 아키텍처의 사이퍼 함수와 S-Box 치환부의 상세한 구성도이다.

<17> 상기 도1을 참조하면, 사이퍼 함수 f 는 32비트의 텍스트 블록을 저장하고 있는 오른쪽레지스터로부터 32비트의 데이터($R(i-1)$)를 입력받아 48비트의 데이터로 확장 치환하는 확장치환부(110)와, 상기 확장치환부의 48비트의 데이터를 입력받고 키 스케줄(Key Schedule)로부터의 보조키(K_i)를 입력받아 배타적 논리합 연산을 수행하는 익스쿠르시브-오아부(120)와, 상기 익스쿠르시브-오아부(120)로부터의 48비트의 데이터를 32비트의 데이터로 대치 치환하는 S-Box 치환부(130)와, 상기 S-Box 치환부(130)의 32비트의 데이터를 복사 치환하는 P-Box 치환부(140)와, 상기 P-Box 치환부의 32비트의 데이터와 왼쪽레지스터에 저장되어 있는 32비트의 데이터($L(i-1)$)를 입력받아 배타적 논리합하는 익스쿠르시브-오아부(150)를 구비한다.

<18> 키 스케줄(Key Schedule)은 56비트의 키(Key)를 입력받아서 28비트의 두 블록으로 나누어서 각각 왼쪽으로 한자리 또는 두자리씩 쉬프트하는 쉬프트부(160, 170)와 상기 쉬프트부의 두 블록을 입력받아 하나의 보조키로 압축하여 치환하는 압축치환부(180)를 구비한다.

<19> 구체적으로, 상기 S-Box 치환부는 48비트의 입력을 받아서 32비트의 출력을 생성하는 8 개의 S-Box로 구성되어 있다. 즉, 48비트의 데이터는 8 개의 6비트 데이터로 분할되어 8 개의 S-Box에 입력된다. 이 8 개의 S-Box들은 8 개의 출력을 내보냄으로써 48 비트를 32비트로 줄인다. S-Box 치환부(130)는 테이블 룩-업(Look-up) 방식으로 대치됨으로써 프로그램가중 논리 어레이(PLA)나 롬(ROM)과 같은 기억장치를 필요로 한다. 6비트의 입력에 대하여 4비트를 출력하기 때문에 각 S-Box는 64×4 의 기억 용량이 필요하며 전체적으로 8개의 S-Box로 구성되어 있으므로 $8 \times 64 \times 4$ 의 기억장치가 필요하다. 따라서 전체적으로 칩에서 차지하는 면적이 상대적으로 크다

- <20> 도2은 처리성능비를 증가시키는 4단의 파이프라인 구조를 갖는 종래기술의 DES 아키텍처이다.
- <21> 상기 도2을 참조하면, 종래기술의 DES 아키텍처는 먼저 초기 치환부를 거친 64비트의 평문(Plain Text) 블록으로 나누어 a_0 와 b_0 를 제1클럭과 제2클럭을 사용하여 각각 제1왼쪽레지스터(A0)(260)와 제1오른쪽레지스터(B0)(200)에 저장한 후 키 스케줄(Key Schedule)로부터 생성된 보조키($K_{(i)}$)를 입력받아 상기 제1오른쪽레지스터로부터의 32비트의 데이터를 사이퍼 함수 $f(210)$ 에 의해서 암호화 변형하며, 상기 사이퍼 함수 f 에 의해 변형된 32비트의 데이터를 상기 제1왼쪽레지스터의 데이터와 익스쿠르시브-오아부(220)에서 배타적 논리합 연산을 수행한다. 또한, 상기 익스쿠르시브-오아부의 32비트 데이터를 제1클럭(CLK1)을 사용하여 제2왼쪽레지스터(A1)(230)에 저장하고, 보조키($K_{(i+1)}$)를 입력받아 상기 제2왼쪽레지스터에 저장되어 있는 32비트의 데이터를 사이퍼 함수 $f(240)$ 를 통하여 변형하며, 변형된 32비트의 데이터를 상기 오른쪽레지스터(B0)(200)의 32비트와 익스쿠르시브-오아부(250)에서 배타적 논리합 연산을 수행한다. 이와 같은 2 개의 라운드가 반복되어 4개의 라운드가 구성되고 마지막 라운드의 제1왼쪽레지스터(A0)(260)의 32비트가 상기 32비트의 블록 b_{15} 가 되며 마지막 라운드의 익스쿠르시브-오아부(270)에서 출력된 32비트가 상기 32비트의 블록 b_{16} 이 된다.
- <22> 상기 제2클럭(CLK2)은 상기 제1클럭(CLK1)을 반전시킨 것으로 상기 제1클럭(CLK1)의 주기의 반만큼 지연시킨 것으로 볼 수 있다. 상기 제1클럭(CLK1)이 상승할 때 상기 왼쪽레지스터 A0와 A1에 새로운 값이 저장되고 상기 제1클럭(CLK1)이 하강할 때 상기 오른쪽레지스터 B0와 B1에 새로운 값이 저장된다.

- <23> 도3은 종래기술에 따른 DES 아키텍처의 동작 순서를 나타내는 타이밍도이다.
- <24> 상기 도3을 참조하면, 32비트의 블록 a_0 와 b_0 는 초기 치환을 거친 64비트의 평문 블록이 32비트의 두블록으로 나뉘어진 것이고, 32비트의 블록 a_0 는 왼쪽변수(L_0)가 되며 32비트의 블록 b_0 는 오른쪽변수(R_0)가 된다. 그리고 DES 코어가 계산하는 값을 b_1, b_2, \dots, b_{16} ($b_i = R_i$)라고 하고 키 스케줄러(Ker Scheduler)가 주기적으로 보조키 K_i 를 사이퍼 함수 f 에 입력해주도록 제어기를 만들면 32비트 블록 b_i 의 값을 계산하는 과정은 다음과 같다.
- <25> 먼저 t_0 와 t_1 에서 a_0 와 b_0 값이 레지스터 A0와 B0에 제1클럭(CLK1)과 제2클럭(CLK2)에 의해서 각각 저장된다. t_1 에서부터 b_1 값($b_1 = a_0 \oplus f(b_0, K_1)$)을 계산하기 시작해서 t_2 에서 계산된 값을 레지스터 A1에 저장한다. 이 때 레지스터 A0에 입력된 값 a_0 는 t_2 까지만 유지가 되면 t_1-t_2 구간에서 b_1 값을 계산하는데 사용할 수 있다. 이 것은 반전된 제1클럭(CLK1)과 제2클럭(CLK2)에 의해서 레지스터 A1과 B0가 새로운 값을 저장하기 때문에 해결할 수 있다. 즉 레지스터 A1이 새로운 데이터를 저장할 수 있는 시간은 t_0, t_2, t_4, \dots 이고 레지스터 B0에 새로운 데이터가 입력되는 시간은 t_1, t_3, t_5, \dots 이다. 마찬가지로 t_1 에서 레지스터 B0에 저장된 값 b_0 와 t_2 에서 레지스터 A1에 저장된 값 b_1 이 t_2-t_3 구간에서 유지되기 때문에 t_3 에서 레지스터 B1에 상기 제2클럭(CLK2)를 사용하여 계산된 b_2 값($b_2 = b_0 \oplus f(b_1, K_1)$)을 저장할 수 있다. 이와 같은 방식으로 상기 제1클럭(CLK1)이 상승할 때 t_4, t_8, t_{12}, t_{16} 에서 계산된 b_3, b_7, b_{11}, b_{15} 값이 레지스터 A0에 저장되고 t_6, t_{10}, t_{14} 에서 새로운 b_5, b_9, b_{13} 의 값이 레지스터 A1에 저장된다. 또한 상기 제2클럭(CLK2)이 상승할 때 레지스터 B0에는 b_4, b_8, b_{12}, b_{16} 값이 t_5, t_9, t_{13}, t_{17} 에서 저장되며, 레지스터 B1에는 b_6, b_{10}, b_{14} 의 값이 t_7, t_{11}, t_{15} 에서 저장된다.

- <26> 도4는 종래기술의 DES 아키텍처의 파이프라인 동작 순서를 나타내는 타이밍도이다.
- <27> 상기 도4을 참조하면, 종래기술의 파이프라인 동작을 나타내는 타이밍도는 파이프라인 구조를 이용하여 두개의 평문 블록들을 8.5클럭 사이클동안 동시에 처리할 수 있음을 보여준다. 또한 도3에서 비어 있는 부분에 새로운 평문 블록 c_0 와 d_0 를 t_2 와 t_3 에서 레지스터 A0와 B0에 입력함으로써 평문 블록 b_i 값들을 계산하는 동안 평문 블록 d_i 값들을 계산할 수 있음을 보여준다. 이 때 t_0-t_1 , t_1-t_2 , t_2-t_3 구간마다 새로운 평문 블록 b_i 와 d_i 값을 암호화 하기위해 사이퍼 함수 f 가 두 개씩 동시에 수행된다. 따라서 사이퍼 함수를 구성하는 S-Box들은 한 개씩 추가로 구현할 필요가 있다.
- <28> 마찬가지로, 4개의 평문 블록을 8.5 클럭 사이클 동안 동시에 처리하기 위하여, 종래 기술의 8 단의 파이프라인 DES 아키텍처에서는 각 시간 구간마다 사이퍼 함수 f 가 네 개씩 동시에 수행된다. 따라서 사이퍼 함수를 구성하는 S-Box들은 네 개씩 추가로 구현할 필요가 있다.
- <29> 도5는 종래기술의 8단의 파이프라인 구조의 DES 아키텍처에서 단일 포트 S-Box 치환부의 구현 방식을 나타낸 상세한 블록도이다.
- <30> 상기 도5을 참조하면, 종래기술의 S-Box 치환부는 네 개를 사용하여 파이프라인 동작을 수행하도록 되어 있고, 하나의 S-Box 치환부는 48비트의 입력 데이터를 받아들여 32비트의 출력 데이터를 내보내는 8 개의 S-Box로 구성되어 있다. 각각의 S-Box는 64×4 의 롬(ROM)이나 프로그램가능 논리 어레이(PLA)로 구성되어 있고 6비트의 어드레스를 입력받아 4비트의 데이터를 출력하는 제1경로(path1)를 구비하고 있다. 네개의 S-Box 치환부에는 서로 다른 제1경로(path1)와 제2경로(path2)와 제3경로(path3)와 제4경로(path4)가 물리적으로 존재한다.

<31> 종래 기술은 상기와 같이 서로 다른 경로가 물리적으로 존재하여 S-Box 치환부를 구현하는데 필요한 기억장치를 동시에 액세스(Access)해야 하는 데이터 컨텐션(Data contention) 문제를 해결한다. 그리고 똑 같은 S-Box 치환부를 네개를 사용하므로 인하여 면적이 증가되는 단점이 있다.

【발명이 이루고자 하는 기술적 과제】

<32> 본 발명은 상기와 같은 종래기술의 문제점을 해결하기 위하여 안출된 것으로서, 액세스(Access) 시간이 네 배 빠른 기억장치를 사용하여 주어진 시간에 데이터를 네 번 액세스하기 때문에 데이터 컨텐션(Contention)을 제거하고 면적을 최소화할 수 있는 암호화 장치를 제공하는데 그 목적이 있다.

【발명의 구성 및 작용】

<33> 상기 목적을 달성하기 위하여 본 발명의 암호화 장치는 데이터 암호화 표준 알고리즘을 사용하여 암호화를 수행하는 암호화 장치에 있어서, 제어기의 제어를 받아 입력되는 네 개의 48비트의 데이터 중에 하나를 선택하는 멀티플렉서; 상기 멀티플렉서에서 출력된 48비트 중에서 6비트의 어드레스 8 개를 입력받아 4비트의 데이터 8 개를 출력하는 8 개의 S-Box; 제어기의 제어를 받아 상기 4비트의 데이터를 네개로 분배하는 디멀티플렉서; 및 제1클럭과 제2클럭을 입력받아 상기 멀티플렉서와 디멀티플렉서를 제어하는 제어기를 포함하여 이루어진다.

<34> 이하, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적

사상을 용이하게 실시할 수 있을 정도로 상세히 설명하기 위하여, 본 발명의 가장 바람직한 실시예를 첨부한 도면을 참조하여 설명하기로 한다.

<35> 도6은 본 발명의 8단의 파이프라인 DES 아키텍처에서 4-포트 S-Box의 구현을 나타낸 블록도이다.

<36> 상기 도6을 참조하면, 본 발명의 S-Box 블록은 제어기의 제어를 받아 입력되는 네 개의 48비트의 데이터 중에 하나를 선택하는 멀티플렉서(610)와, 상기 멀티플렉서(610)에서 출력된 48비트 중에서 6비트의 어드레스 8 개를 입력받아 4비트의 데이터 8 개를 출력하는 8 개의 S-Box(620)와, 제어기의 제어를 받아 상기 4비트의 데이터를 네개로 분배하는 디멀티플렉서(630)와, 제1클럭(CLK_A)과 제2클럭(CLK_B)을 입력받아 상기 멀티플렉서와 디멀티플렉서를 제어하는 제어기(640)를 구비한다.

<37> 도7은 종래의 단일 포트 S-Box와 본 발명의 4-포트 S-Box의 동작을 나타내는 타이밍도이다.

<38> 상기 도7을 참조하면, 본 발명에서는 제어기에 입력되는 네 배가 빠른 제1클럭(CLK_A)과 제2클럭(CLK_B)을 이용하여 롬(ROM)을 액세스(Access)하는데 필요한 신호들을 발생시킨다. 각 시간 구간 t_i-t_{i+1} 에서 제1경로(path1)와 제2경로(path2)와 제3경로(path3)와 제4경로(path4) 중의 한 경로를 선택하는 멀티플렉서에 의해 시분할된 제1경로(path1)와 제2경로(path2)와 제3경로(path3)와 제4경로(path4)가 개념적으로 존재하여 데이터 컨텐션(Data Contention) 문제를 해결한다.

<39> 도7에 도시된 바와 같이 t_7-t_8 구간에서 b_7, d_5, f_3, h_1 을 계산하기 위해서 4 번 S-Box를 시분할 하여 액세스(Access)함을 보여준다. 각 시간 구간 t_i-t_{i+1} 에서 4 개의 경

로 중에서 어떤 경로를 선택하는 것은 멀티플렉서와 디멀티플렉서를 제어하는 제어기의 구현 방식에 의존한다. 제어기에 입력되는 두 배 빠른 제1클럭(CLK_A)과 제2클럭(CLK_B)은 롬(ROM)을 액세스(Access)하는데 필요한 신호들을 발생시키기 위한 기준이 된다.

<40> 본 발명의 기술 사상은 상기 바람직한 실시예에 따라 구체적으로 기술되었으나 상기한 실시예는 그 설명을 위한 것이며 그 제한을 위한 것이 아님을 주의하여야 한다. 또한, 본 발명의 기술 분야의 통상의 전문가라면 본 발명의 기술 사상의 범위내에서 다양한 실시예가 가능함을 이해할 수 있을 것이다.

【발명의 효과】

<41> 상기와 같이 본 발명은 S-Box를 한 개만 사용함으로써 S-Box가 차지하는 면적을 종래기술에 비해 1/4로 축소하였다. 또한 여러 형태의 DES 아키텍처를 구현하여 성능과 면적을 최적화 할 수 있는 선택의 범위를 증대시킨다.

【특허청구범위】**【청구항 1】**

데이터 암호화 표준 알고리즘을 사용하여 암호화를 수행하는 암호화 장치에
있어서,

제어기의 제어를 받아 입력되는 네 개의 48비트의 데이터 중에 하나를 선택하는
멀티플렉서;

상기 멀티플렉서에서 출력된 48비트 중에서 6비트의 어드레스 8 개를 입력받아 4비
트의 데이터 8 개를 출력하는 8 개의 S-Box;

제어기의 제어를 받아 상기 4비트의 데이터를 네개로 분배하는 디멀티플렉서; 및
제1클럭과 제2클럭을 입력받아 상기 멀티플렉서와 디멀티플렉서를 제어하는 제어기
를 포함하여 이루어진 암호화 장치.

【청구항 2】

제 1 항에 있어서,

상기 제1클럭과 제2클럭은 서로 반전된 신호임을 특징으로 하는 암호화 장치.

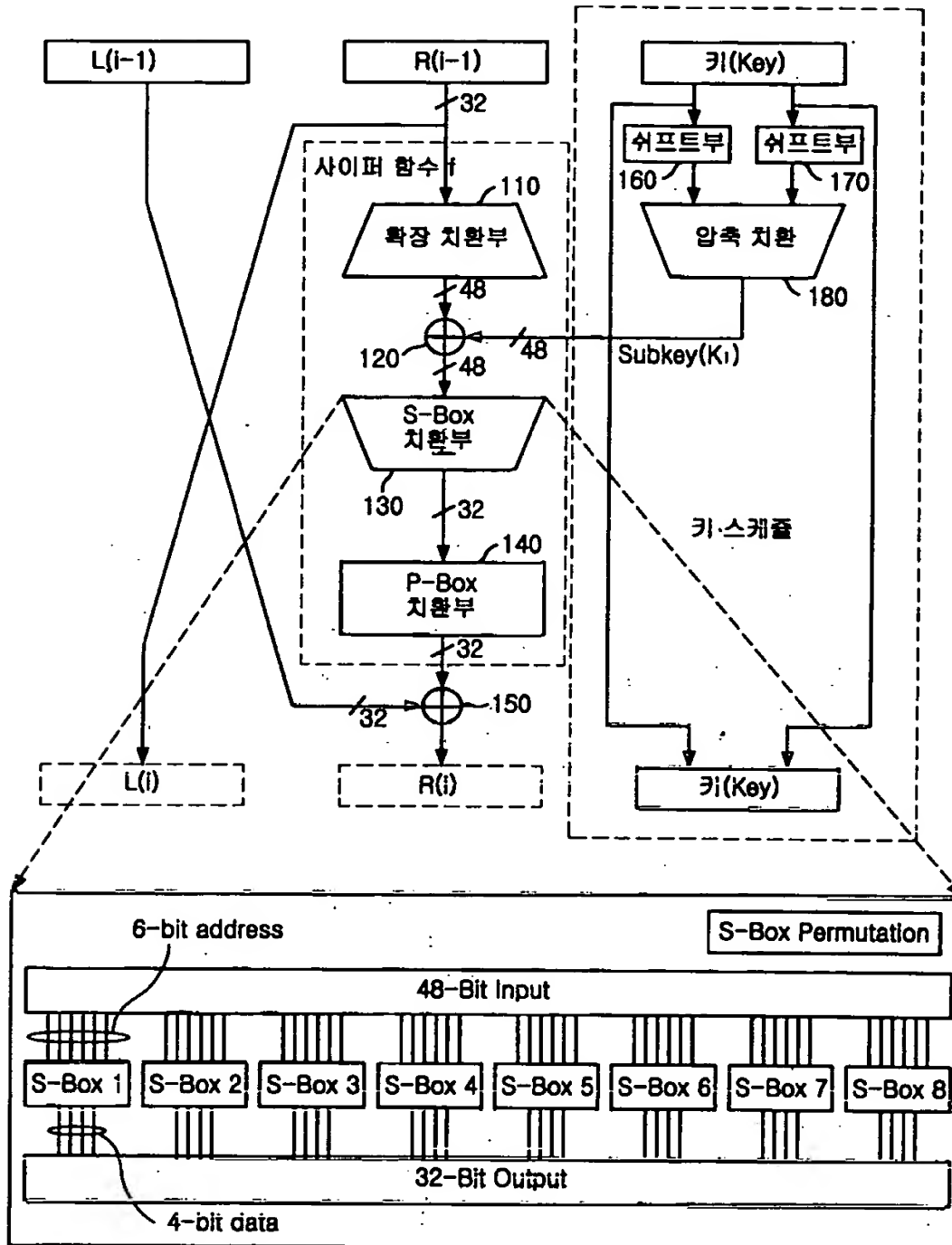
【청구항 3】

제 1 항에 있어서,

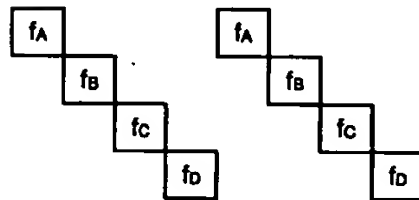
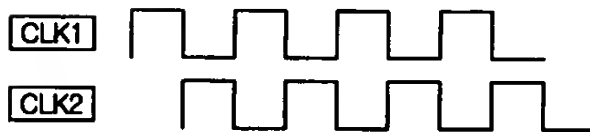
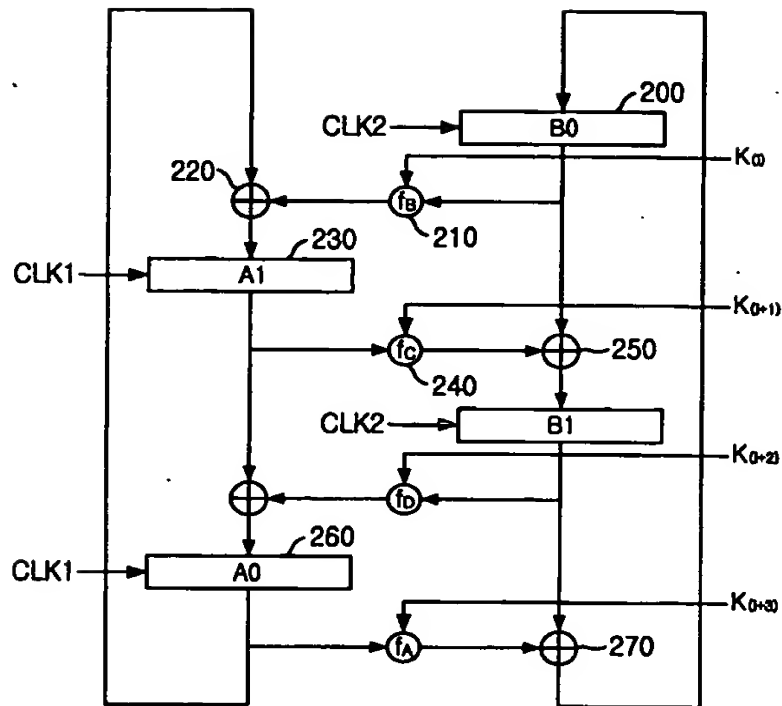
상기 멀티플렉서와 디멀티플렉서는 물리적으로 존재하는 네 개의 입력과 출력 경로를 시
분할하여 데이터의 충돌을 방지하는 것임을 특징으로 하는 암호화 장치.

【도면】

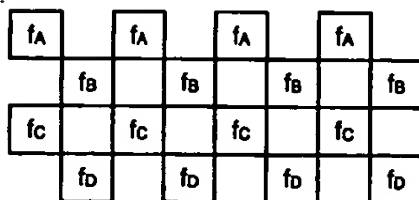
【도 1】



【도 2】

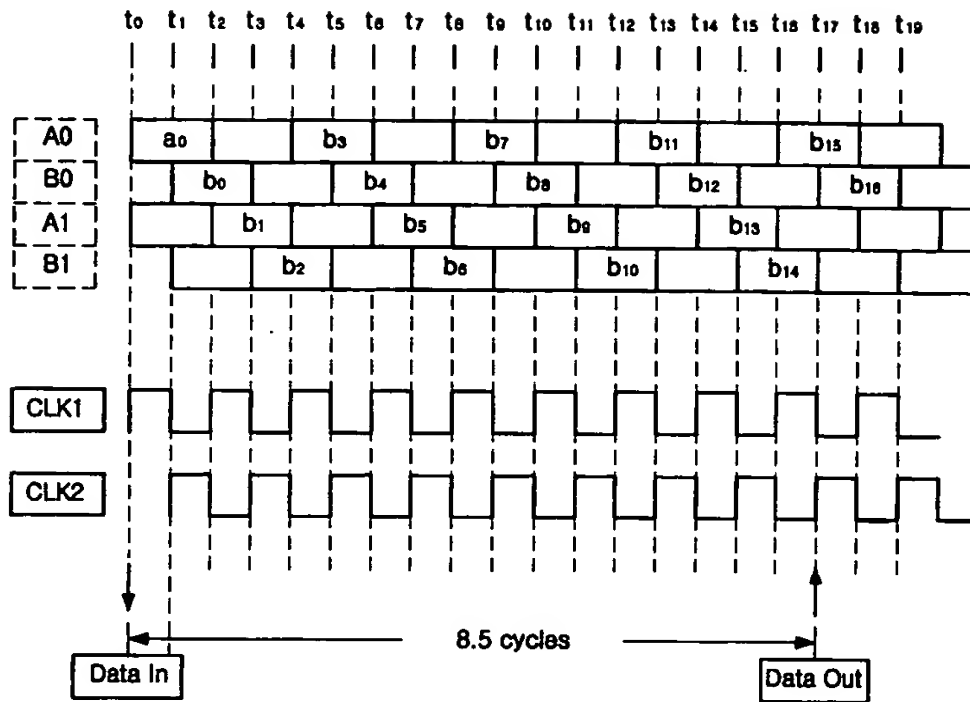


*파이프라인을 사용하지 않은 경우

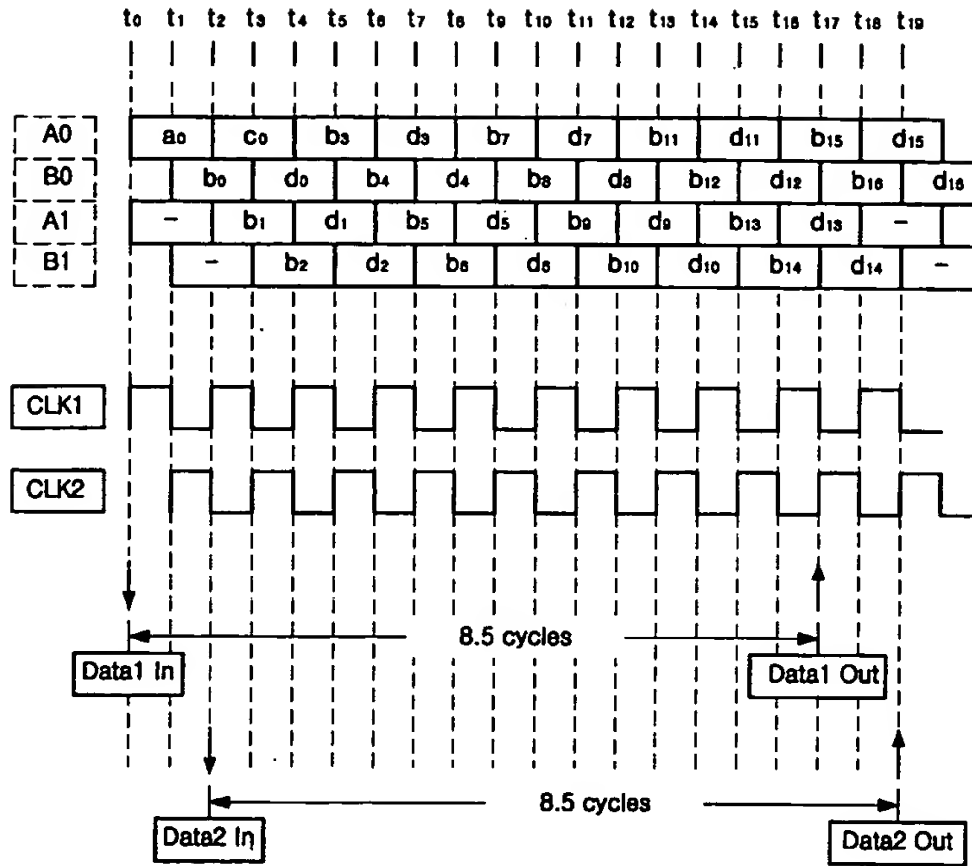


*파이프라인을 사용하는 경우

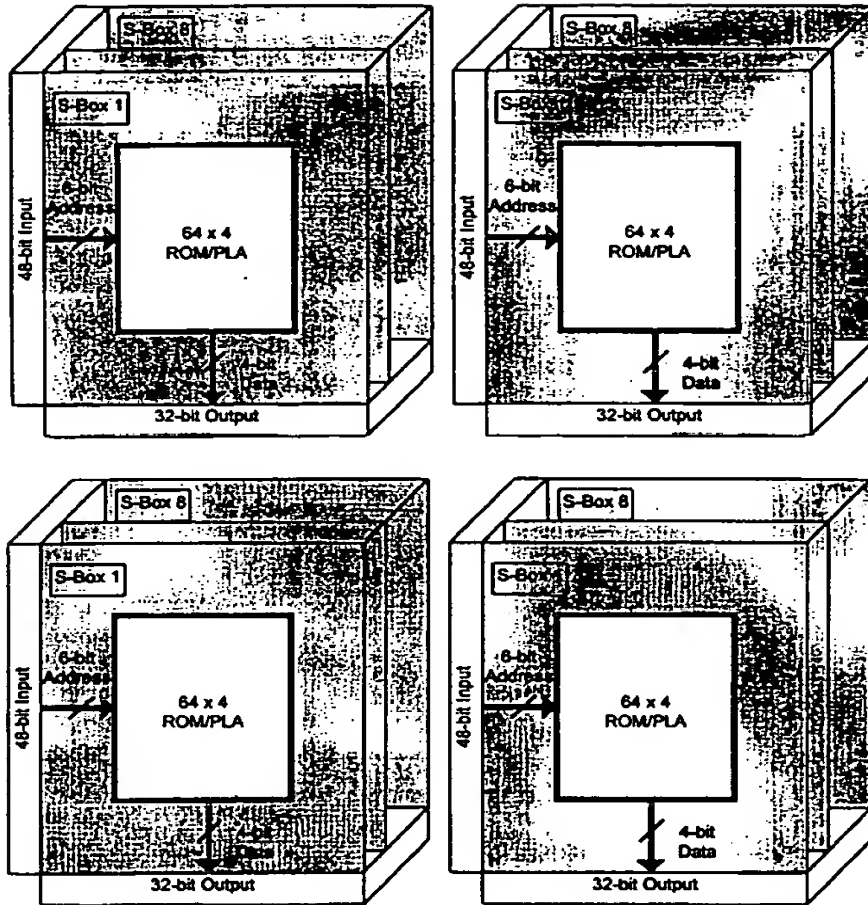
【도 3】



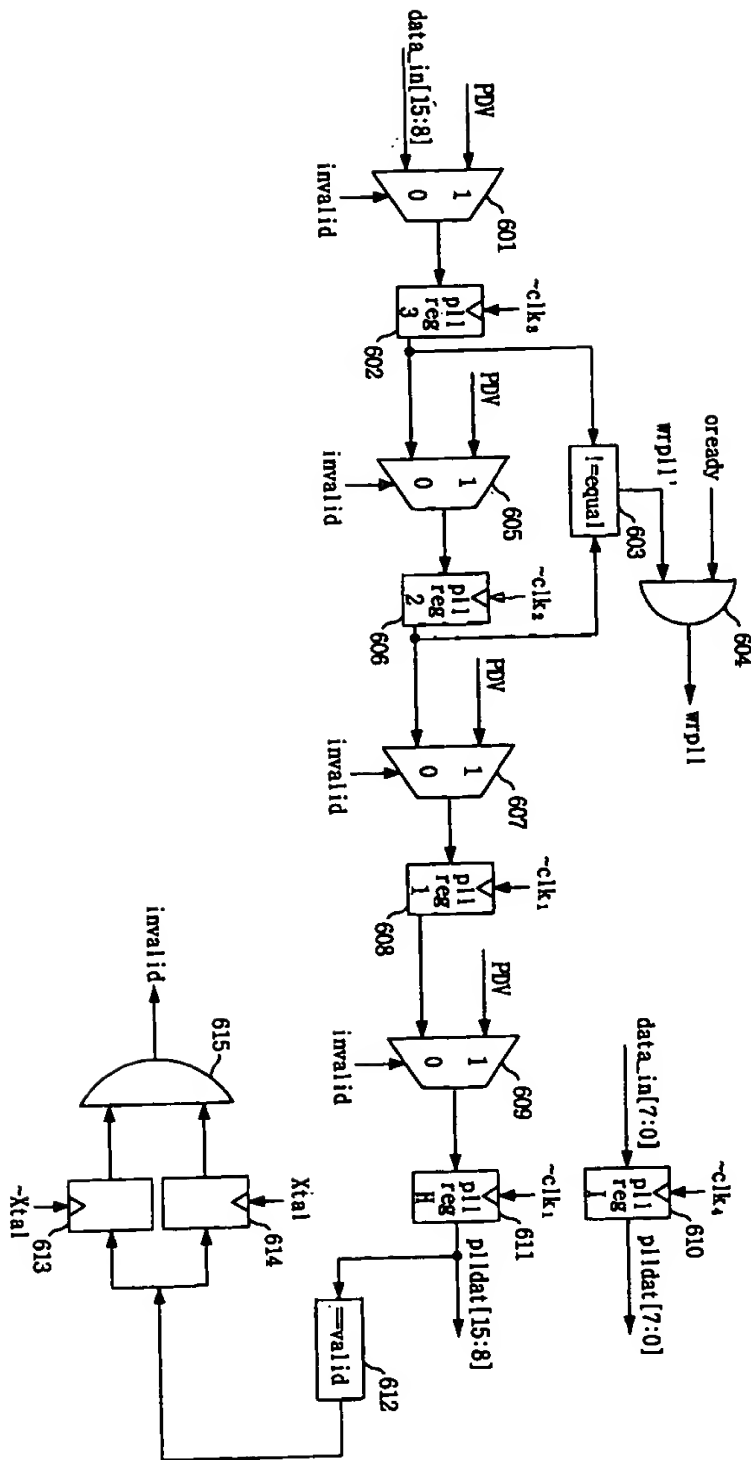
【도 4】



【도 5】



【도 6】



【도 7】

